CLEARTOKEN

White Paper

The Case for a Central Securities Depository for Digital Assets

Chapter One:

The Settlement Challenge

March 2025

The Settlement Challenge in Digital Assets

Financial markets depend on **secure, efficient, and legally final settlement** to function effectively.

In traditional finance (TradFi), **post-trade infrastructure ensures that assets and cash are exchanged simultaneously**, mitigating counterparty risk and ensuring market stability.

In **digital asset markets**, this foundation is missing.

Despite the promise of blockchain technology, today's digital asset real-time gross settlement (RTGS) models **reintroduce risks that financial markets have spent decades eliminating**.

In particular, the absence of **delivery vs payment (DvP) settlement** through **regulated financial market infrastructure (FMI), such as a central securities depository (CSD)** leaves participants exposed to counterparty, liquidity, and systemic risks.

While proponents of **atomic settlement** claim that blockchain can eliminate these issues, real-world constraints (including liquidity fragmentation, prefunding requirements, and regulatory uncertainty) demonstrate that **settlement finality and risk mitigation require structured market infrastructure, not just faster technology**.

This paper explores the critical need for a regulated digital asset CSD, particularly in off-chain settlement, while also highlighting key risks and inefficiencies in on-chain settlement.

This first chapter explores why digital asset markets need a regulated **digital CSD** to ensure **secure, efficient, and scalable settlement** to enable the institutional adoption and growth of digital asset markets.

Chapter Summary

1 **Digital asset markets lack the regulated infrastructure needed for institutional adoption.**

Unlike traditional markets, there is no regulated CSD to co-ordinate settlement manage risk and ensure trade completion.

2 **The absence of regulated delivery vs payment (DvP) settlement exposes participants to significant risks**

Without synchronised asset and cash exchange, digital asset markets remain vulnerable to counterparty, liquidity, and systemic risks.

3 **Off-chain settlement is dominant but centralises risk in unregulated entities.**

While off-chain models offer speed and efficiency, they lack transparency, require high prefunding, and expose participants to counterparty and systemic risks.

4 **On-chain settlement introduces operational and liquidity challenges.**

Block time delays, network congestion, and liquidity fragmentation undermine its reliability, making real-time settlement unpredictable and capital-intensive.

5 **Atomic settlement does not eliminate risk and is not a complete solution.**

Prefunding, lack of netting, and cross-chain coordination issues limit its scalability and practicality for institutional adoption.

6 **A digital CSD is essential to bridging on-chain and off-chain settlement.**

By harmonising traditional financial safeguards with blockchain innovation, a digital CSD enables true DvP, risk mitigation, and market scalability.

Everything Is Fine, Until It Isn't:
Lessons from Settlement Failures

Settlement risk is not a new problem. History has repeatedly shown that unsynchronised, free of payment (FoP) settlement models lead to systemic failures. The collapse of Bankhaus Herstatt in 1974 and the Wormhole bridge hack in 2022 illustrate how failures in settlement coordination can result in significant financial losses and market instability.

Herstatt Risk: When Settlement is Unsynchronised

26th June 1974: Seattle First National Bank delivered $22.5m in Deutschmarks to Bankhaus Herstatt[3-1] (worth $145m today[3-2]), expecting to receive US dollars in return. Hours later, regulators shut Herstatt down after uncovering irredeemable losses from excessive foreign exchange risk exposure (at least 470m Deutschmarks[3-3], equivalent to €846.5m today[3-4]). Seattle First National, and many other US banks, were left without the hundreds of millions of US dollars they were owed.

Despite German authorities downplaying the relatively small West German bank's collapse as a "local accident", it severely threatened international market stability with widespread repercussions. **Counterparty trust collapsed**. Small banks were shunned in favour of the largest and most trusted institutions. New York became wary of sending dollars to Europe. The bank's owner and several employees were later convicted of fraud.[3-5]

Herstatt's collapse triggered a global rethink of financial settlement processes, exposing failures in market self-regulation and regulatory oversight. It also illuminated what is now known as "***Herstatt risk***", the settlement risk arising from one party delivering its obligations while the counterparty's payment is still pending, and could fail, in another time zone. **Herstatt risk is typical of unsynchronised, FoP settlement in which counterparties are left exposed to financial loss when a trade fails mid-process.**

The Wormhole Hack: A Digital Take on FoP Risk

2nd February 2022: 120,000 ETH worth $325m was stolen from the major DeFi blockchain bridging protocol, Wormhole, which creates interoperability between the 6 most popular blockchains through smart contracts. Users send cryptocurrency to Wormhole which triggers its smart contracts to issue a 'wrapped' representation of the token for use on another blockchain.

The attack targeted the Ethereum-Solana bridge. It exploited a vulnerability in its trust assumptions which assumed reserves to be present without real-time verification. This allowed wrapped ETH (wETH) to be minted on Solana without first verifying the necessary 1:1 collateral on Ethereum. The result? The Ethereum leg of the hacker's transaction of the transaction failed, yet the Solana leg (wETH issuance) continued.[3-6]

The hacker subsequently moved their unbacked wETH back to Ethereum; a process in which Wormhole burned the wETH tokens and credited the hacker with the equivalent ETH, which they withdrew. This left Wormhole users holding 120,000 of unbacked wETH on Solana, while the corresponding Ethereum reserves were already gone, exposing them to a one-sided default**.** This was only prevented by Jump Trading, Wormhole's parent company, injecting $325 million to restore the lost ETH backing and making its users whole.[3-7]

Wormhole's model relied on trusting that the bridge would always function correctly. That assumption failed when the system was exploited. It functioned as an FoP settlement system: assets on one blockchain were transferred to users based on assumptions instead of simultaneous confirmation and synchronised transfers.

The Lesson for the Future of Digital Asset Markets

Though 50 years apart with differences in assets and technology, both the Herstatt and Wormhole failures demonstrate the **fundamental flaw of FoP settlement: assets are delivered on trust, not certainty.** At its core, Herstatt risk arises when one party delivers assets before receiving value in return; an issue magnified in markets where transactions span across different jurisdictions, time zones, or, indeed, blockchains.

Never Assume What Should be Certain

FoP settlement assumes eventual completion, but this is not guaranteed. Much like Herstatt's creditors who never received the U.S. dollars they were owed *after* sending Deutschemarks, Wormhole users were left holding unbacked wETH when the Ethereum leg failed *after* they had sent ETH. Without Jump's intervention to restore the lost collateral, their users would have been left with worthless tokens, just as Herstatt's FX counterparties were left with worthless positions when the bank collapsed.

In trading relationships with high trust, FoP can offer flexibility to meet settlement obligations, but it introduces significant risks when adopted at scale. Without structured DvP settlement, participants are exposed to counterparty risk and any failure to meet settlement obligations can trigger broader financial instability. To mitigate this, safeguards such as credit limits, collateralisation, or structured risk management frameworks must be in place.

Different Assets, Same Problem

Both Herstatt and Wormhole highlight the fundamental need for intermediated settlement infrastructure. **Whereas TradFi rectified this exposure through FMI, digital asset markets still lack this safeguard today.** Wormhole's breach wasn't just another exploit; it was a structural failure in the way digital assets are settled across blockchains.

A digital CSD bridges this gap, ensuring that digital assets benefit from the same safeguards that have made traditional financial markets resilient for decades. in the absence of a trusted intermediary ensuring synchronised settlement, FoP-based digital asset transfers are highly vulnerable to the same systemic failures that historically destabilised traditional finance.

The Solution: Delivery vs Payment Settlement

Settlement failure, whether from errors, attacks, or deliberate strategy, is common and must be actively mitigated. In a market with unsynchronised settlement, a single failure can trigger a domino effect across multiple counterparties, amplifying systemic risk, as we have seen.

DvP Relies on Immobilisation & Intermediaries

The DvP settlement model ensures the immobilisation of assets and their synchronised exchange through a trusted intermediary. DvP settlement system operators are typically regulated intermediary FMIs such as CSDs and in FX markets CLS Group provides a payment versus payment (PvP) mechanism.

Settlement system operators ensure that assets and cash are immobilised and when both sides are verified, they simultaneously settle between the buyer and seller. This eliminates vulnerabilities typical of FoP settlement (including Herstatt risk), mitigates counterparty and credit risk and protects counterparties from systemic failures. As a result, DvP settlement is a cornerstone of financial markets, underpinning trillions of dollars in daily transactions.

Unregulated and Fragmented Market Structure

Digital asset markets currently operate without the safeguard of regulated market infrastructure to deliver DvP settlement. Instead, they rely on fragmented and unsynchronised processes, typically operating through unstructured, loosely regulated financial infrastructure. This creates vulnerabilities to many of the risks that traditional financial markets worked hard to eliminate. The absence of proper controls, risk management, and transparency allows centralised risk and systemic weaknesses to go largely unchecked.

High-profile market failures underscore the need for robust DvP settlement mechanisms and infrastructure, and the same regulatory standards that traditional markets rely on, to protect investors and ensure market stability. This makes DvP an essential pillar to ensuring strong financial markets.

However, decentralised finance (DeFi) is designed to eliminate intermediaries, making consistent market implementation of DvP challenging. While emerging solutions such as smart contract-based escrow mechanisms and atomic settlement attempt to replicate DvP, they remain incomplete without the governance, oversight, and risk management provided by trusted intermediaries. For example, Wormhole operated in an escrow-style manner which failed to truly implement DvP. For example, had Wormhole implemented more robust DvP mechanisms to operate at the time of issuing wrapped ETH, wETH issuance would have not been possible without having immobilised ETH in hand.

Code Alone Cannot Supersede Legally Backed Market Structure

Technology can help enforce conditional transactions, but it cannot ensure systemic stability, legal finality, or regulatory compliance on its own. Regulated market structure and enforceable risk management frameworks are critical to ensuring market stability and protecting against cascading failures.

The consequences of these structural weaknesses have played out in multiple high-profile failures. Three Arrows Capital, for example, took on substantial amount of unsecured or under-secured loans from lenders like Celsius and Voyager, ultimately defaulting and contributing to their subsequent collapses. This lack of robust safeguards and risk controls created contagion across the crypto lending space, exacerbating systemic instability.

All Financial Markets Are Built On Trust

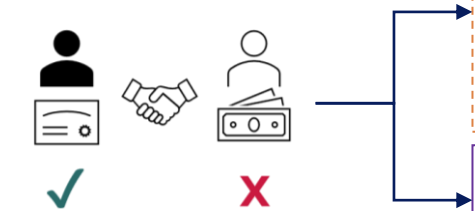
For financial markets to function efficiently and securely, settlement infrastructure must be robust, enforceable, and trusted by all participants.

Despite blockchain protocols being designed to be 'trustless' at the base layer, transacting across different networks, asset types, and market structures still requires trust and intermediation to effect settlement.

The digital asset market's reliance on bridging protocols, Layer 2 networks, and centralised exchanges introduces dependencies on unregulated intermediaries and technical mechanisms that, if compromised, can create single points of failure.

Just as traditional finance relies on regulated FMIs for risk mitigation, **digital asset markets require purpose-built, accountable intermediaries to deliver true DvP that the market can trust in**. Without this, they risk repeating the same failures that plagued pre-regulated financial markets, only this time, on-chain.

Intermediated Delivery vs Payment Is Critical for Mitigating the Effects of Counterparty Default



A trade is executed in which the seller delivers their assets, but the buyer does not deliver the cash.

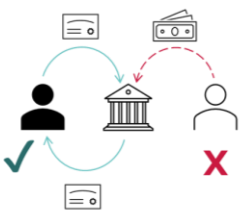
Free of Payment Without DvP

(Higher Risk)

Free of payment settlement is entirely based on trusting your trading counterparty to deliver what they promise. The seller delivered first and will not receive what they were owed.

With a CSD Operating DvP

(Lower Risk)



CSDs ensure that cash and assets are released simultaneously once both sides have been received. If the buyer defaults, the seller has their assets returned by the CSD

An Unsynchronised Step Backwards:
Technology Alone Cannot Eliminate Settlement Failure

Blockchain technology can eliminate settlement risk through the concept of "atomic settlement". This is the enforcement of instant trade execution, which theoretically, should result in the simultaneous settlement of both trade legs, carrying out DvP.

However, given the differing settlement rails underpinning significant volumes of cryptoasset vs fiat trading pairs, the need to solve settlement finality through technical and legal frameworks is becoming increasingly important.

On-Chain Settlement

- Transfer of value occurs through direct validation on blockchain by consensus.
- Each transaction is settled individually on a real-time gross settlement (RTGS) model without netting.
- Blockchain records are immutable and cannot be altered without great difficulty.
- Dependence on smart contracts to effect ***atomic settlement*** on the same or different chains.
- Challenges include high prefunding requirements, liquidity fragmentation, unpredictable 'finality' and reliance on smart contracts.

Off-Chain Settlement

- Trading operates through centralised trading platforms (CEXs), custodians or bilateral arrangements
- These parties manage balances and conduct any necessary on-chain transfers (e.g. moving from a custodian's wallet to participant wallet is an on-chain transaction).
- Models vary but typically on-chain transactions only happen when assets/funds need to leave or enter a system.
- Settlement inter and intra-blockchain are not necessarily contingent on each other.
- Introduces counterparty risk, requiring trust in intermediaries who typically hold assets or collateral.

Whilst both models make claims to providing DvP settlement, neither model is immune from risk. Each model comes with trade-offs compared to settlement through a centralised, regulated entity ensuring DvP settlement typical of TradFi. First, we will look at typical off-chain settlement.

Centralisation in a Decentralised Financial System: A New Source of Risk

CEXs typically use off-chain settlement to settle trading activity with their customers. Unlike on-chain settlement, which individually records and validates transactions on a blockchain network, off-chain settlement updates balances within a centralised system without an immediate blockchain transaction.

There are many benefits to off-chain settlement, including:

- **Instant balance updates:** no waiting for on-chain validation, e.g. block confirmations.
- **Greater predictability:** avoids erratic blockchain gas fees and network congestion.
- **More efficient liquidity management** through netting and margin trading.
- **Integration** with existing financial infrastructure.

Prefunding Requirements Create Capital Inefficiency

A major challenge in off-chain settlement is the high prefunding requirements imposed by most exchanges. Since there is no regulated central counterparty or CSD to legally guarantee trades, participants must **fully collateralise their positions before trading**, tying up significant capital.

This is particularly problematic for institutional participants, as it reduces capital efficiency, increases liquidity constraints, and limits the ability to deploy assets elsewhere. Unlike TradFi, where CCPs enable margining and netting to optimise liquidity, most off-chain digital asset venues **demand 100%+ prefunding** to mitigate their own counterparty risks. This creates a capital drain, making large-scale institutional participation less viable.

The Risk of Centralised Exposure in an Unregulated Environment

The high prefunding requirements in off-chain settlement do not eliminate risk, they simply shift it.

Unlike in regulated markets, where CCPs, CSDs, and regulatory oversight mitigate systemic failures, off-chain settlement today relies entirely on the solvency and risk management of individual platforms. Risks include:

- **Lack of Regulation & Offshore Exposure:** Many major CEXs and custodians operate offshore, outside of robust regulatory oversight. Users are often exposed to **arbitrary rule changes, liquidity crises, and mismanagement**, with limited legal recourse.
- **Counterparty Risk:** Participants must **trust the platform to honour balances and withdrawals**. If the custodian or exchange becomes insolvent, users may be unable to recover their assets.
- **Settlement Completion Uncertainty:** Because no blockchain transaction is recorded until assets are withdrawn, users rely entirely on **the solvency and risk management** of the platform to ensure their settlement obligations due are honoured.
- **Single Points of Failure:** Centralised platforms can be hacked, suffer liquidity shortfalls, or collapse due to poor risk management.
- **Hidden Liabilities & Lack of Transparency:** Off-chain balances are not auditable in real time, making it difficult to detect insolvency risks before they materialise. Many failures occur because platforms misrepresent their financial health, with no public ledger to verify their claims.

Risk is Being Concentrated

This creates concentrated risk within a handful of centralised entities, such as custodians, prime brokers, and exchanges. If a trading venue **collapses, becomes insolvent or is otherwise compromised,** prefunded assets may be **locked or lost**.

This lack of transparency, governance, and enforceable risk controls has led to repeated failures. Examples like FTX's collapse and Celsius' insolvency demonstrate the danger of entrusting prefunded assets to platforms without regulatory safeguards. When these entities fail, customers become unsecured creditors, facing lengthy legal battles with little recourse. The recent Bybit hack (see right) is an example of how **custodian-level on-chain movements exposed users to security breaches.**

Bybit Hack: February 2024

A new record was set for the largest crypto theft when over $1.4 billion in assets was stolen from crypto exchange Bybit in a major security breach that exploited weaknesses in its transaction approval processes.[6-1]

The attack underscored a critical weakness in digital asset markets: decentralisation forces centralised functions at crypto exchanges: they act as custodians and settlement agents which is not the case for TradFi trading venues.

As a result, users are at risk of bearing the full brunt of counterparty failure, whether due to hacking, mismanagement, or insolvency.

Fortunately for Bybit users, the exchange was able to secure emergency funding to restore its reserves. They are unlikely to recover the stolen tokens.[6-2]

The Bybit incident highlights the ongoing vulnerabilities in digital asset markets and reinforces the urgent need for robust, institutional-grade settlement infrastructure.

The absence of standardised risk management, capital buffers, and segregation of client funds exacerbates these issues, creating a fragile market structure where liquidity crises, mismanagement, or fraudulent activity can trigger systemic contagion.

This highlights the urgent need for **regulated market infrastructure** that can provide **risk-mitigated, efficient settlement solutions** without excessive prefunding burdens.

Off-chain settlement is essential for institutional adoption but carries significant risks due to **a lack of regulation, counterparty exposure, and reliance on opaque offshore entities**. The solution is not to eliminate off-chain settlement but to **improve it with regulated, transparent, and risk-mitigated infrastructure**—a role that a **digital CSD can fill**.

On Again, Off Again… The Link Between On-Chain and Off-Chain Settlement

Despite the risks of off-chain settlement, institutions rely on it due to the impracticalities of relying on on-chain settlement alone and for its speed and efficiency in a fragmented market. However, on-chain activity remains an essential component of off-chain settlement.

When participants need to **deposit, withdraw, or transfer assets between platforms**, an **on-chain transaction is required**.

Additionally, on-chain movements establish ownership on decentralised networks, providing transparency and auditability, ensuring that assets exist and are not simply IOUs on an opaque balance sheet. For example, a trader executing multiple trades on a CEX will see their balance update instantly within the exchange's ledger. However, no on-chain transaction occurs until they withdraw their funds to an external wallet. This could be managed by the CEX or their custodian.

These on-chain movements introduce **new risks**, especially if the custodian or exchange handling them is compromised. Instead, a regulated digital CSD is needed to bridge the gap. This can ensure that both on-chain and off-chain settlement occur within a structured, transparent, and risk-mitigated framework that protects market participants, granting legal certainty over asset ownership and settlement finality.

We will now explore the risks of on-chain settlement to understand why neither model can fully replace traditional market infrastructure in solving the fundamental challenges of digital asset market settlement.

Analysing the Atomic Axiom: Exploring the Realities of On-Chain Settlement

Now, let's examine on-chain settlement, characterised by its atomic settlement model. There is no universally accepted definition, but **atomic settlement is generally characterised by two key properties:**

Simultaneity	&	**Instantaneity**
Transactions are executed on "an all-or-nothing" basis		Settlement occurs immediately after trade execution

Atomic settlement relies on programmable smart contracts to ensure trades execute upon pre-defined conditions being met. **Once initiated, the settlement process cannot be interrupted, amended, or reversed.** As such, atomic settlement is often promoted as the intermediary-free solution to resolving counterparty risk, completing trades within seconds and instantly freeing capital; unlike TradFi's T+1/T+2 settlement cycles.

Can Atomic Settlement Deliver True DvP?

At first glance, this mirrors traditional DvP settlement. Blockchain technology eliminates the need for both intermediaries and the delay between execution and settlement (i.e. settlement cycles).

Proponents argue this approach prevents settlement failure since trades only execute if both parties hold the required assets. Theoretically, this eliminates settlement risk and the need for regulated oversight, all whilst increasing capital velocity. This fuels expectations that blockchain will ultimately replace intermediaries like central counterparty/clearing house (CCPs) and CSDs.

In practice, however, it introduces significant operational, liquidity and systemic risks that financial markets have long worked to mitigate. **By settling trades individually on a gross basis**, atomic settlement removes the CCP role in netting and margining trades, shifting risk onto market participants.

However, digital asset markets are not immune from settlement failure or delays between execution and settlement as **atomic settlement is not truly simultaneous.** It only functions instantly if all transactions occur on the same blockchain and execute via a smart contract. In reality, most digital asset trades span multiple chains, platforms, and off-chain components, creating settlement exposure. For example, the most traded pair is BTC/USDT, requiring settlement on two different chains.

Post-Execution, Trade Legs Are Disconnected

Even if both legs of a transaction are initiated at the same time, counterparties are still exposed to risk until assets are received into their wallet or tokenised cash is off-ramped back into fiat currency through traditional banking infrastructure. Without blockchain-based central bank money, the cash leg remains disconnected, slowing settlement and increasing risk. This fragmentation introduces new challenges absent in TradFi.

Ironically, 'Instant' Settlement Depends on Block Time

Blockchain is often positioned as enabling real-time settlement, making assets available instantly. In fact, **block time** introduces **inherent delays** between trade execution and settlement, challenging the notion of 'instant' settlement.

For a transaction to be considered "final", (meaning that is complete, irrevocable, and unsusceptible to double spending), it must be recorded in a block and followed by a chain of 'confirmation blocks'. The required number of confirmations vary by protocol, but they are necessary for reaching settlement consensus. Rather than depending on legal validity, 'finality' is judged to be the point of consensus, at which it is mathematically improbable to alter the chain and reverse the transaction.

Settlement Should Run Like Clockwork

This process creates an undefined settlement window, introducing risks rather than eliminating them. For example, Bitcoin requires six confirmation blocks. With an average block time of 10 minutes,[7-1] settlement takes at least one hour. Block times are inconsistent: in the 12 months prior to December 2024, Bitcoin's daily average first-block confirmation times ranged from 20 minutes to nearly 18 days with a median of 2 hours.[7-2]

Whilst some other blockchains operate faster, settlement is only as fast as the slowest network component. Network congestion, node performance, and consensus mechanisms all impact settlement times The longer it takes to reach settlement consensus, the longer the window of risk.

Latency Risk

A congested network or delays in block creation introduce **latency risks**, which are compounded when transactions occur across multiple chains. While Layer 2 solutions can improve transaction speed and cost efficiency on individual blockchains, they do not inherently solve cross-chain co-ordination challenges, which remain a persistent barrier to achieving real-time settlement.

This **undefined settlement window** creates risks for institutions that rely on predictable, time-bound processes. With no third-party risk mitigation, market stability relies entirely on the technology consistently operating as expected, every time. This introduces significant operational risk. Unlike TradFi, where CSDs **immobilise assets and synchronise the exchange** of cash and securities, blockchain-based settlement leaves assets in limbo until 'finality' is established.

Why This Matters for Institutional Adoption

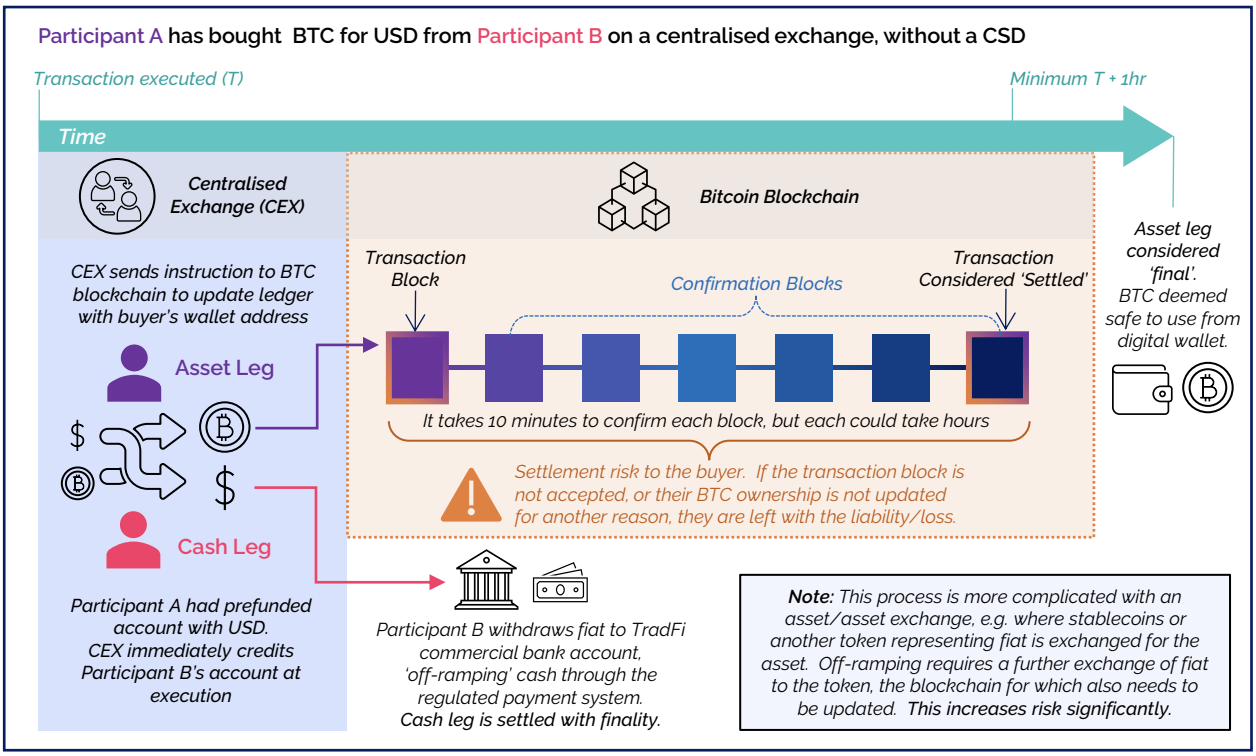
For institutions moving large volumes, these delays introduce:

- **Liquidity risk:** Assets remain locked while waiting for settlement confirmation.
- **Operational inefficiencies:** Firms must monitor multiple chains for finality instead of a centralised clearing process.
- **Counterparty risk:** Uncertainty around when (or if) settlement will complete creates exposure, especially in cross-chain transactions.

Block time constraints highlight why institutions **prefer off-chain settlement**. Without a mechanism to **immobilise assets and synchronise cash movements**, blockchain-based real-time settlement does not provide the certainty required for regulated markets.

A digital CSD solves this by ensuring that assets are immobilised, and settlement is executed under structured, regulated conditions, eliminating reliance on unpredictable blockchain settlement while maintaining interoperability with on-chain networks.

Simultaneous Settlement Instructions Does Not Mean Simultaneous Settlement Is Achieved
(Simplified Illustration)



The Illusion of Atomic DvP: Why Real-Time Isn't Risk-Free

While promising, atomic settlement application remains complex and dependent on network conditions and protocol design. Whilst true atomic settlement occurs on-chain when smart contracts enforce instant, indivisible settlement, off-chain solutions can approximate atomic settlement but often require trust in an intermediary or deferred settlement finality. During the unspecified settlement window, assets remain tied up for multiple confirmations before they can be considered safe to use, creating risk exposure to counterparty, operational and market risks.

Therefore, despite claims of achieving DvP solely through atomic settlement, such transactions are inherently settled through FoP. **Settlement instructions can be sent simultaneously, but without an intermediary or trust mechanism to enforce simultaneous exchange, payments and asset transfers occur independently.**

This means that the settlement ***instructions*** may be co-ordinated, but the actual ***delivery*** of obligations is not.

Settlement risk goes beyond ensuring both sides of the trade receive what they expect. Instant settlement is not a universal solution to regulatory concerns; in fact, DLT presents additional challenges that could contribute to systemic risk.

The Realities of Real-Time Aren't So Rosy: The Pitfalls of Real-Time Settlement

The Intensity of High Transaction Volumes

Real-time gross settlement places significant demands on distributed ledger technology (DLT), requiring it to execute transactions consistently under all conditions, even during periods of extreme stress, 24/7, 365 days a year. However, decentralisation introduces inherent limitations to network performance.

Nodes, which enable decentralisation. must individually verify and record transactions, creating an operational burden that slows down processing. Since network speed is dictated by the slowest node, blockchain systems tend to operate at significantly lower speeds than traditional financial market infrastructures.

Processing Speeds Are Critical

Most established financial market infrastructures can process tens of thousands of transactions per second (TPS) with near-zero latency. For example, the US securities CSD, DTCC, processes peak volumes up to 25,000 transactions per second[9-1] and Visa can process up to 65,000 transactions per second.[9-2]

Some blockchains fall far short of this benchmark, but others have high TPS volumes that will need to be tested against stress test conditions experienced by traditional systems. Maximum theoretical TPS vary considerably by chain:[9-3]

- *Bitcoin – 7*
- *Ethereum – 119*
- *Avalanche – 1,191 (often reported as 6,500)*
- *Polkadot – 10,000*
- *Solana – 65,000*
- *SUI – 300,000*[9-4]

Beyond TPS, on-chain settlement introduces latency due to block time and network congestion. Transactions on Bitcoin typically require 10 minutes to complete a block, while Ethereum blocks range between 10-19 seconds depending on network conditions.[9-5] As discussed, settlement 'finality' requires multiple block confirmations, meaning actual completion times can be much longer. During periods of network congestion, delays increase, and transaction fees rise as users compete for block space, further slowing down the settlement process.

TPS Illustrates Just Part of the Picture

While TPS is often used to compare blockchain networks, it lacks standardisation across the ecosystem. Different platforms define TPS differently: some count simple token transfers, while others include complex smart contract executions, making direct comparisons unreliable. Furthermore, many reported TPS figures reflect ideal conditions rather than real-world constraints like congestion, latency, and security overhead. Without a standardised method of measurement, TPS remains an incomplete benchmark for blockchain scalability.

Scalability constraints and uncertainty are particularly problematic in securities markets, where daily transaction volumes routinely reach hundreds of millions, far beyond the capacity of current blockchain solutions. At times of high demand, network congestion increases block time, and settlement costs. This makes RTGS impractical to satisfy trading at an institutional scale.

To enable digital asset markets to grow and compete with traditional financial systems, the dependency on RTGS must be eliminated in favour of intermediated settlement. A centralised digital CSD can consolidate and co-ordinate workflows, ensuring the high throughput, seamless settlement, and operational efficiency that securities markets require.

Comparing Transaction Volumes In US Securities and Bitcoin Markets

	US Securities NSCC Jan- Dec 2023 [9-6]	**bitcoin** Dec 2023 - Dec 2024 [9-7]
Average daily transactions (gross)	197.1 million	0.53 million
Annual total transactions (gross)	49,669 million	193 million
Trading Days	252	364

The Complexity of Interoperability & Integration

Interoperability remains a fundamental challenge in the digital asset ecosystem due to the proliferation of blockchains, creating self-contained silos of activity and liquidity. The lack of standardisation across protocols leads to significant hurdles in network synchronisation and interaction. For example:

- Smart contracts are not universally supported across blockchain protocols.
- Different blockchains use distinct programming languages.
- Consensus mechanisms vary, affecting transaction validation.
- Data architectures differ, creating incompatibilities.
- No uniform standards exist for cross-chain bridging solutions or smart contract validation.
- Inconsistent network fee structures.

Attempts to bridge disparate blockchains introduce additional complexity, operational risks, and security vulnerabilities, ultimately increasing settlement and liquidity risks in the pursuit of cross-market atomic settlement.

The risks of interoperability failures are significant. As demonstrated by the Wormhole exploitation, cross-platform vulnerabilities can be exploited, creating security risks, liquidity fragmentation, and operational inefficiencies.

A significant amount of effort is being spent retrofitting blockchain protocols to meet the stringent requirements of capital markets; tasks they were not originally designed for. While blockchain technology is often promoted as a way to eliminate FMIs, in practice, unregulated intermediaries are being relied upon to facilitate cross-market solutions, with none of the oversight or accountability of a regulated FMI.

Moreover, interoperability challenges extend beyond DLT networks to legacy financial systems. While firms would ideally integrate digital asset activity alongside their traditional operations, failures are more likely to stem from DLT connections to outdated IT architecture.

Building enterprise-grade infrastructure to support digital transformation will require substantial financial, technological, and expert resources. It will also necessitate rigorous development, testing, and integration of new in-house systems, along with enhanced monitoring and surveillance capabilities to meet regulatory requirements.

bZx Oracle Manipulation Attack

In February 2020, bZx, a decentralised lending and margin trading platform, was exploited due to its reliance on a vulnerable price oracle from Kyber Network. The attack manipulated asset prices to extract unearned profits, leaving bZx out of pocket.

The attacker took a **7,500 ETH (~$1.98M) flash loan**, using **3,518 ETH (~$939K)** to buy **sUSD**, a synthetic USD stablecoin, which they posted as collateral. To inflate its value, they used **900 ETH (~$240K)** to artificially push sUSD's price to **$2** through Kyber Network's price feed. Since bZx's smart contract relied on this oracle, it accepted the manipulated price as valid.

With the inflated collateral, the attacker borrowed **6,796 ETH (~$1.8M)**, repaid the flash loan, and walked away with **2,378 ETH (~$635K) in profit**. Once the price returned to normal, bZx was left with a shortfall.

The entire exploit took under a minute, highlighting the risks of using unaudited or single-source price oracles in DeFi protocols.[10-2]

The Reality of Liquidity Management

The most immediate challenge of real-time settlement is liquidity management. Immediate settlement near-eliminates exposure to market movement and price volatility. However, without the settlement window to align the correct cash or securities at the time required, participants must have all resources in place at the moment of trade execution.

Prefunding requirements tie up liquidity, making markets less efficient and less attractive to participants. Market instability, volatility, or external geopolitical events could increase prefunding needs, causing knock-on settlement failures.

The absence of CCPs and CSDs in digital assets results in 100% prefunding requirements by trading venues, as no intermediary provides margin or organises settlement.

This requirement could increase systemic risk, particularly in markets with high interconnectivity and dependency on liquidity. As seen in other contexts, such as the US T+1 transition, reducing settlement cycles requires careful coordination across payment systems, collateral management, and operational workflows.

Additionally, eliminating settlement cycles removes netting mechanisms that enhance market efficiency by offsetting exposures across multiple trades. Without settlement cycles, firms must fund every trade individually, significantly increasing liquidity demands. Atomic, real-time settlement actually exacerbates operational risks rather than mitigate them.

Blockchain does not inherently solve fundamental market risks, particularly in the absence of an integrated cash settlement mechanism as we will discuss shortly.

The Necessity of Settlement Cycles

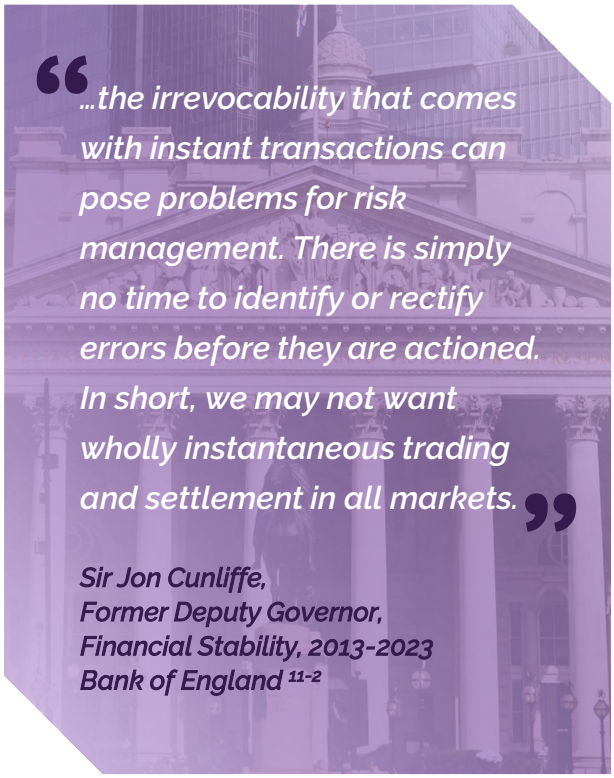
While blockchain-based atomic settlement offers a compelling vision of efficiency, the assumption that 'faster is always better' ignores the fact that financial stability depends on structured processes that ensure market integrity. Financial markets already operate at extraordinary speed, with electronic trade execution occurring in nanoseconds. The typical 1-2 day settlement cycle exists because it mitigates risk through the post-trade processes (including trade validation, clearing, and settlement) which involve sequential steps carried out by multiple participants and intermediaries including CCPs and CSDs.

Settlement windows will always exist, even if only for fractions of a second. On blockchain, that period is undefined and open to risk as clearance to use assets is determined by confirmation block-based probability rather than the certainty of settlement finality in a known timeframe.

If evaluating "risk as a function of time",[11-1] reducing the time between trade execution and settlement seems like a logical way to reduce risk. However, the rigidity of atomic, real-time settlement introduces new risks that could outweigh its perceived benefits.

In this context, the selling point of blockchain irrevocability is also a threat: the immediate and permanent execution of trades provides no opportunity to identify or correct errors before they are executed. This makes it complex or potentially impossible to fix errors, for example:

- **Smart contract vulnerabilities**: Bugs, loopholes, or bad-faith construction in smart contracts can be exploited, with no way to alter them once deployed. The lack of testing, regulatory maturity and accountability makes this an unpredictable technology to put 100% faith in, certainly at this stage. Their security flaws are a serious threat for theft and manipulation. Smart contracts, whilst being a vehicle for automation and simplicity, cannot just be left to run themselves from a legal nor a technical perspective. There are very real technical vulnerabilities that are exacerbated by attempts to enforce cross-chain interoperability.
- **Oracle dependencies**: If external data feeds (oracles) provide incorrect or compromised information, incorrect actions may be executed irrevocably (see box below). They act as a single source of truth, becoming a single point of failure.
- **Unforeseen execution:** Terms could be set in smart contracts that are executed due to unexpected issues, volatility or defaults which were not foreseen during the smart contract's creation, leading to a chain of events which may not be able to be stopped.
- **Lack of governance:** There is little opportunity to challenge theft or errors unless an incident is severe enough for the platform's community to agree to unwind transactions by rolling back the blockchain. Such incidents question the purpose of DLT as the cornerstone of decentralised finance. For example, disagreements on how to resolve the DAO exploitation on Ethereum that resulted in a loss of $60m ETH led to the 2016 fork, splitting the blockchain into Ethereum and Ethereum Classic.



By contrast, settlement cycles in TradFi serve a **critical function beyond just timing**: they provide a structured buffer for trade validation, error resolution, and risk mitigation. **Real-time settlement eliminates this safeguard**, forcing participants to fully prefund trades and increasing liquidity demands.

Rather than an inefficiency to be eliminated, the gap between execution and settlement is an essential risk-management mechanism, ensuring that financial markets function smoothly without unnecessary capital strain.

Crucially, settlement cycles enable netting, allowing multiple trades to be consolidated into a single, reduced settlement obligation. This dramatically lowers the number of required payments and asset movements, freeing up liquidity and reducing systemic risk. Without netting, each trade must be settled individually, amplifying operational and liquidity burdens, **a challenge that digital asset markets must address as they scale**.

Real-Time Eliminates Netting Benefits & Efficiencies:
Bilateral RTGS Cannot Compress Cross-Market Settlement Obligations

In order to facilitate DvP settlement, the settlement system operator/CSD receives trading data from all its participants. This creates a unique opportunity to employ trade compression, or netting, mechanisms that consolidate multiple transactions into a single net obligation, thereby reducing the number of settlements and associated risks.

There are **two key forms of netting**: clearing netting and settlement netting.

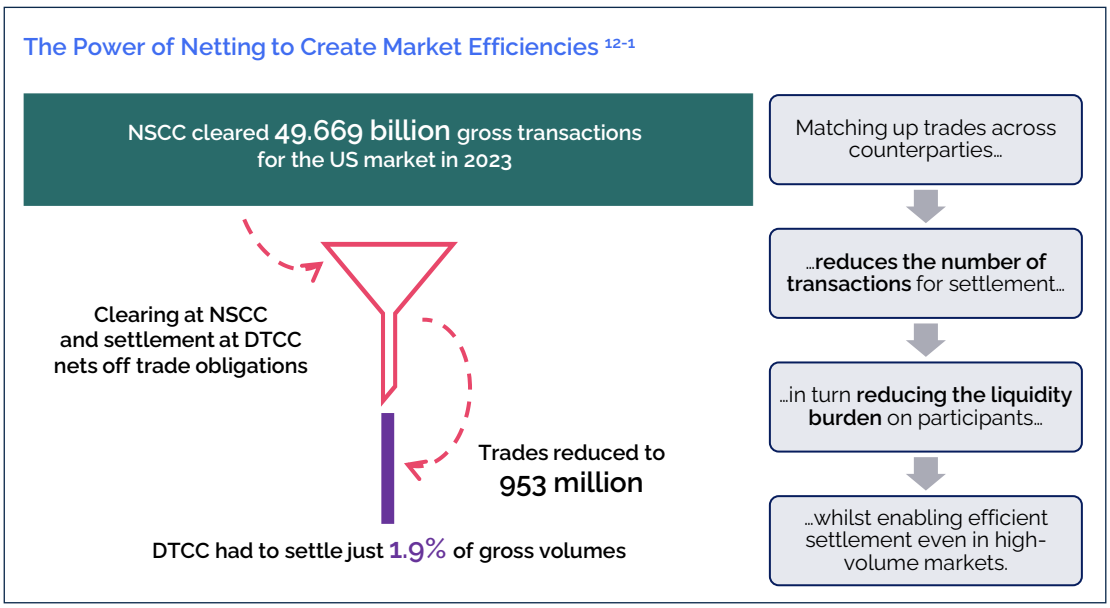
Clearing netting (CCP):

- The CCP interposes itself between trade participants, legally becoming the buyer to every seller and the seller to every buyer.
- It aggregates all exposures; offsetting buy and sell obligations to reduce counterparty risk and margin requirements.
- This significantly reduces the number of outstanding contractual obligations between market participants and margin requirements, optimising capital efficiency.

Settlement netting (CSD):

- Takes place at the final stage of a transaction lifecycle, typically by a CSD.
- Netting consolidates obligations from all CCPs and any other sources into a single net delivery per security and a single net cash payment per counterparty at the end of a settlement cycle.
- This reduces liquidity demands and ensures that the settlement process remains efficient and cost-effective.

While clearing netting reduces counterparty risk and operational complexity, settlement netting ensures the actual movement of securities and cash is minimised, optimising the use of liquidity and reducing systemic risk in financial markets. For example, in the US securities markets netting reduced transaction settlements by 98.1%:



The efficiency netting brings is vital in high-volume securities markets. However, the digital asset market is built upon bilateral arrangements requiring individual settlement. As we have seen, especially in times of rapid market growth such as the paperwork crises of the late 20th century, there is a point at which gross settlement processes fails to scale, creating a crisis.

Netting is fundamental to DvP settlement as it reduces the total number of payments and deliveries required: the more transactions there are to settle, the higher the risks (settlement, operational, credit), costs (transaction, settlement), inefficiencies (capital, market) and potential for error (reconciliation).

Without a settlement window or a mechanism to facilitate netting, real-time gross settlement (RTGS) requires fully funded positions for every transaction, creating significant liquidity challenges. Prefunding requirements often exceed 100%, leading to severe liquidity constraints.

The need to settle every transaction individually increases friction, tying up liquidity and placing unnecessary capital burdens on participants. The fragmented nature of digital asset markets only exacerbates this problem, as multiple platforms operate in isolation without a mechanism for aggregate risk reduction. There is a clear need for central coordination to aggregate obligations and improve efficiency, however developers are reworking protocol designs and creating Layer 2 solutions to emulate the centralised clearing and settlement systems that TradFi has enjoyed for decades.

We Must Avoid A New 'Digital Paperwork Crisis'

We are at risk of creating a new 'digital paperwork crisis' if we do not heed the lessons of the past. Just as markets struggled with inefficiencies prior to the introduction of netting and clearing houses, today's digital markets are facing similar constraints. This is not a problem of technology: without scalable infrastructure to create the opportunity for cross-market netting mechanisms, the sheer volume of bilateral transactions in a growing market will lead to increased costs, trapped liquidity, and operational bottlenecks.

A robust netting mechanism is essential to prevent market gridlock. The ability to reduce settlement obligations, free up capital, and mitigate systemic risk is what enabled traditional financial markets to scale effectively. The same principles must now be applied to digital securities markets through the establishment of a DvP settlement system and CSD for digital assets.

The Paperwork Crises: A Warning from History

Trading electronification, deregulation and increased market participation led to trading volumes surging in both London and New York in the late 20th century, yet settlement processes remained manual, dependent on paper certificates, physical ledgers, and clerks shuttling documents between institutions on a gross basis. The system could not keep pace, buckling under the weight of its own growth.

The New York crisis peaked in 1968 when daily trade volumes quadrupled from 3 million shares in 1960 to 12 million. Clerical staff struggled to process transactions, leading to massive backlogs, delayed settlements, lost securities, and operational chaos. To manage the crisis, the NYSE was forced to shorten trading hours, close on Wednesdays, and extend the settlement cycle from T+4 to T+5. More than 100 brokerage firms collapsed under the strain, exposing the fragility of gross settlement—where each trade required a separate exchange of cash and securities without a mechanism for netting obligations efficiently.

Two decades later, London experienced a similar upheaval following the 'Big Bang' deregulation in 1986 in which trading volumes surged by 60% in just one week. Settlement inefficiencies led to escalating counterparty risk, frequent trade failures, and market gridlock.

Lessons Learned: The Birth of Modern Market Infrastructure

Both crises underscored the urgent need for automated, centralised infrastructure. The fallout led to the creation of CSDs, automated settlement systems, and netting mechanisms that form the backbone of today's financial markets. Prior to these reforms, settlement operated on a FoP basis with long settlement windows, allowing risk to escalate amidst confusion. The 'nuts and bolts' of post-trade processes, once overlooked, became a critical area of focus to ensure financial stability.

Avoiding a New Digital Paperwork Crisis

History has shown that fragmented and inefficient settlement processes cannot scale. Today's digital asset markets, built on bilateral gross settlement, risk repeating the same mistakes. Without robust netting and infrastructure, markets face unnecessary capital burdens, trapped liquidity, and systemic inefficiencies. The lesson is clear: scalable infrastructure is not optional—it is essential to prevent market gridlock and financial instability.

***Read more about the Paperwork Crises, the origins of CSDs and post-trade reform in our first white paper: "Bridging the TradFi-DeFi Gap:** The Future of Finance Depends on Traditional Trust and Regulation".*

Central Bank Ledger Integration:
Cash is Not a Digital Asset, DvP Needs Central Bank Integration

Blockchains cannot directly settle fiat currency within regulated banking frameworks: the cash leg of a trade is another hurdle for atomic settlement to deliver true DvP.

Traditional financial markets ensure synchronised settlement of both the asset and cash legs through infrastructure integrated with central bank ledgers. In contrast, **blockchains cannot directly settle both the cash and asset legs of a trade**, instead fragmenting these two components. This increases risk particularly on the cash leg, where tokenised assets must often be converted back into fiat.

The 'Singleness of Money' Does Not Yet Apply to DLT

Traditional fiat currency systems rely on centralised ledgers maintained by central and commercial banks. Reconciliation between payment and settlement systems guarantees accuracy across all ledgers. Transactions are finalised through ledger adjustments, ensuring seamless cash settlement. However, this "singleness of money", where all forms of money are interchangeable, does not extend to DLT, as there is no form of digital money with the stability, legal backing, and interoperability inherent in central bank money.

Whilst assets can be tokenised and recorded on blockchain, fiat currency remains external to these systems due to legal and operational constraints. This prevents direct on-chain settlement of cash transactions. Although stablecoins and digital tokens attempt to replicate fiat currency on blockchain, they lack the legal status, regulatory oversight, and direct liquidity of central bank money, introducing counterparty and systemic risks.

Legally, only banks can hold cash deposits, meaning that fiat currency cannot be custodied but must be deposited within a regulated banking framework. For example, Article 40 of the EU CSDR requires CSDs to settle cash payments through central bank accounts or otherwise regulated commercial banking services. As a result, **atomic real-time settlement alone cannot achieve DvP in a legally robust manner without intermediary support**.

Legal Settlement Finality Depends on Meeting Legal Requirements

Cash must remain within a regulated banking framework to maintain the legal certainty of settlement finality; a critical concept that we will explore further in the paper. Blockchain alone cannot guarantee settlement finality, which must apply to both asset and cash legs to protect trades from the knock-on effects of counterparty insolvency and transaction 'unpicking'. Without this, systemic risks multiply, threatening market stability.

Until a fungible, central bank-backed digital currency can be used on blockchain, the cash leg in digital asset trades will remain a bottleneck, introducing risks and inefficiencies.

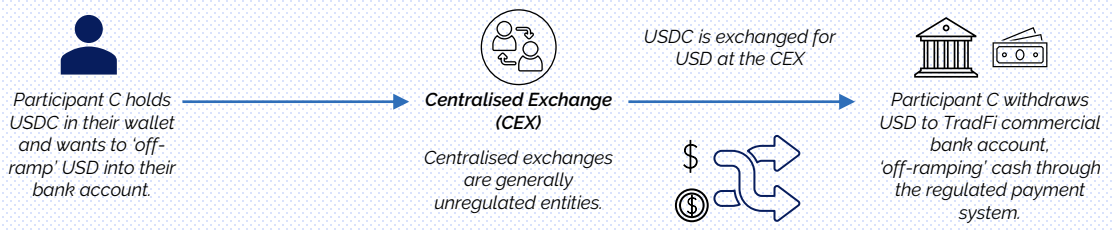
The On-Ramp / Off-Ramp Problem: Ramps = Risk

As central bank-backed fiat money does not exist natively on any DLT protocol, participants must use intermediaries (e.g., crypto exchanges, trading platforms, prime brokers, or specialist custodians) to "on-ramp" fiat into the DeFi ecosystem by converting it into cryptocurrencies, stablecoins, or other tokens which are stored in their own digital wallet. This process introduces transaction fees, settlement risk, and exposure to intermediary insolvency.

This limitation exacerbates risk, as additional transactions are required at cryptocurrency exchanges to convert deposit tokens into fiat and then off-ramp the fiat into a bank account to complete the trade. A participant could transfer their digital asset to the buyer but fail to retrieve their cash due to the lack of direct coordination between the trade's legs.

Conversely, "off-ramping" fiat back from digital assets into cash also requires intermediary co-ordination, adding further complexity, cost, and risk. Unlike traditional finance, where CSDs simultaneously deliver cash and assets on standard settlement cycles, the digital asset ecosystem lacks synchronised, standardised DvP mechanisms.

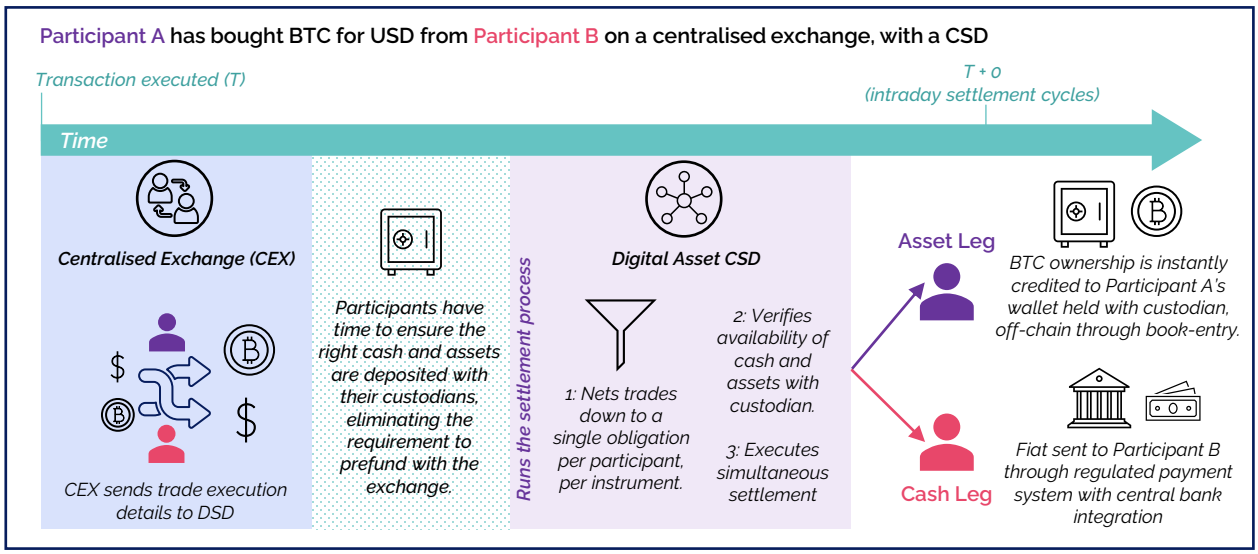
Off-Ramping Crypto into Fiat Currency (*Simplified Illustration*)



This disconnect results in inefficiencies and risks. While a digital asset can settle on its blockchain, the seller may still face delays or failures when extracting fiat from the system. A co-ordinated mechanism for settling both the cash and asset legs is indispensable for reducing systemic risks, highlighting the necessity of intermediated settlement for digital asset markets.

The foreign exchange (FX) market faced a similar challenge. Initially focused on mitigating currency fluctuation risks, Bankhaus Herstatt's aforementioned collapse demonstrated the need for an independent intermediary to facilitate simultaneous payment vs payment (PvP) settlement. These mechanisms were critical in reducing post-trade and systemic risks. Just as the FX market required PvP mechanisms to mitigate systemic risk, digital asset markets must adopt a similar model for legally sound and operationally robust DvP settlement.

A Digital Asset CSD Can Facilitate True DvP and Maintain Netting Efficiencies *(Simplified Illustration)*



Tokenising Cash: A Future Path Forward?

The tokenisation of cash is often positioned as a key enabler of seamless DvP in digital asset markets. Digital representations of fiat currency, backed 1-to-1 by central or commercial banks, could take the form of wholesale or synthetic central bank digital currencies (CBDCs) respectively.

In this model, as in TradFi, central banks would maintain a centralised ledger of deposits, transactions, and balances, which would interoperate with commercial bank ledgers.

The Potential of Central Bank Digital Currencies

CBDCs offer the potential to eliminate the inefficiencies and risks associated with on/off-ramping fiat within digital asset markets. Wholesale or synthetic CBDCs would preserve the singleness of money across physical, electronic, and digital formats. Unlike stablecoins, tokenised fiat would carry legal equivalence to fiat, enabling seamless, regulated, and reliable cash legs in digital asset transactions.

However, It is unlikely that central banks will create an open, interoperable cash settlement layer for all market participants (for example, public blockchains), nor that such a solution will be available in every currency. Most tokenised cash solutions are expected to operate within closed, permissioned networks of regulated institutions, preventing universal availability.

We Already Have A Solution

So, the fundamental challenge remains; true DvP requires cash settlement that is accessible, final, and legally robust across different asset classes, market structures and jurisdictions. Regulatory frameworks have solved for this, requiring DvP settlement systems to be operated by regulated "synchronisation operators", typically, CSDs.

The need for a regulated CSD for digital assets remains clear. By integrating with both digital asset ledgers and central bank ledgers, a digital asset CSD ensures simultaneous updates whereby both sides of a trades settle together, or not at all, whilst guaranteeing settlement finality on a 24/7 basis. This would bridge the current gap between fiat and digital assets, delivering operational resilience and unlocking the true potential of digital finance.

Achieving True DvP Settlement:
Opening the Case for a CSD for Digital Assets

The evolution of financial markets has consistently demonstrated that DvP settlement enabled by safe and scalable infrastructure is essential for stability and growth. Without structured market infrastructure, digital assets remain vulnerable to the same risks that led to past financial crises.

Blockchain-based, real-time atomic settlement is often positioned as the ultimate solution for financial market efficiency, providing an instant and risk-free solution. **However, as we have examined, the practical reality is far more complex.** Blockchain's intermediary-free, bilateral RTGS model presents significant structural challenges that remain unsolved, overlooking key incompatibilities and risks, resulting in amplifying, rather than solving, existing market inefficiencies.

A digital asset CSD is the critical missing link. Functioning similarly to a traditional CSD to deliver DvP, it will connect digital asset ledgers with central bank-backed money, synchronising the simultaneous exchange of cash and digital assets under legally binding terms. By providing the proven safeguards that institutions and regulators require, the market will benefit from mitigated counterparty risk and strengthened systemic stability.

A Digital Asset CSD Can Resolve Current On-Chain and Off-Chain Settlement Challenges

Blockchain Settlement Challenges	Digital CSD Solutions
Atomic settlement synchronising settlement instructions but failing to simultaneously deliver assets and cash.	**Delivery vs Payment (DvP)** synchronising simultaneous asset and cash exchanges
Real-time settlement elimination of settlement cycles and with them, the buffers to rectify errors or organise capital	**Optimised intraday settlement cycles** More frequent T+0 settlement cycles on a 24/7 basis.
Prefunding and liquidity lock-up Requiring fully funded positions makes markets less efficient.	**Optimised liquidity** Netting and margining mechanisms lower capital requirements and improve risk management
No netting Every trade settles individually, increasing costs, transaction volume and prefunding requirements.	**Netting mechanisms** Reduce settlement costs and transaction volume.
Absence of tokenised fiat currency two steps to on or off-ramp fiat into the system	**Integration with central bank ledgers** able to simultaneously and instantly deliver the cash leg
Scalability issues Cannot efficiently support institutional trading volumes with unpredictable settlement timing and costs	**Institutional-grade scalability** Supports high-volume transactions and integration with TradFi.
Bilateral counterparty risk No intermediary to manage counterparty exposure or default risk.	**Counterparty risk mitigation** Centralised netting and default protections reduce exposure.
Interoperability challenges Different blockchains operate in silos, preventing seamless settlement and increasing risk.	**Seamless cross-market integration:** Overcome interoperability issues and silos
Intensive technology and compliance requirements incompatible for direct integration with institutions' highly regulated, legacy IT systems.	**Seamless market integration** integrates with existing financial infrastructure, reducing market participants' operational and cost burden.
Legal uncertainty No established framework for legal finality and insolvency protection,	**Legal finality** Legal finality is recognised and enforceable under existing regulations.

The Market is Not Ready for Real-Time

A move to real-time settlement would not just be a technical upgrade for financial participants but a fundamental restructuring of market infrastructure, risk management models, and liquidity frameworks. As regulators have warned, real-time settlement may "negatively impact liquidity, price formation, and the ability of financial markets to absorb supply or demand shocks." Every part of this highly interdependent system would need to be perfectly synchronised, leaving no room for error; something that today's markets are simply not designed to accommodate.

TradFi operates on legacy technology, complex back-office processes, and stringent regulatory frameworks that are not built for real-time settlement. Even incremental shifts, such as the move from T+2 to T+1, require extensive coordination across payment systems, collateral management, and operational workflows. The absence of uniform standards across networks means that immediate settlement risks errors, delays, and discrepancies in balance sheets, a problem that is only amplified in an environment with fragmented protocols.

Nor Is the Market Ready for Direct Blockchain Integration

The assumption that smart contracts can fully replace traditional settlement processes overlooks the significant ongoing cost and complexity of maintaining, monitoring and auditing them at an institutional scale to ensure security and compliance. Considerable computational resources are also required to processes blockchain-based transactions, which can introduce settlement delays rather than eliminating them.

Institutional infrastructure must meet rigorous operational and regulatory standards, but smart contracts introduce new risks: from code vulnerabilities to single points of failure. For example, around 85% of Ethereum nodes run on Geth, making software diversity a key regulatory concern.[17-1]

"A Bridge Too Far"?

While blockchain-based settlement is often framed as the future of financial markets, the reality is far more complex, a fact acknowledged by a market expert who called **real-time settlement is "a bridge too far"** as it needs "everything [to] work perfectly in a world where there's still people involved".[17-2] This view is reinforced by industry sentiment: recognised by a recent survey in which 44% of respondents were "somewhat concerned" and 28% "very concerned" about the EU moving to T+0 settlement.[17-3]

A CSD for digital assets resolves these challenges by harmonising proven TradFi settlement models with digital innovation. Rather than forcing a market-wide shift to real-time settlement, a digital asset CSD provides a scalable, resilient framework that ensures finality, compliance, and interoperability across market participants, 24/7, 365 days a year.

Institutional Adoption Depends on Trusted FMI

The future of digital asset settlement **must combine innovation with structured, regulated infrastructure**, and not simply discard the mechanisms that have safeguarded financial markets for decades.

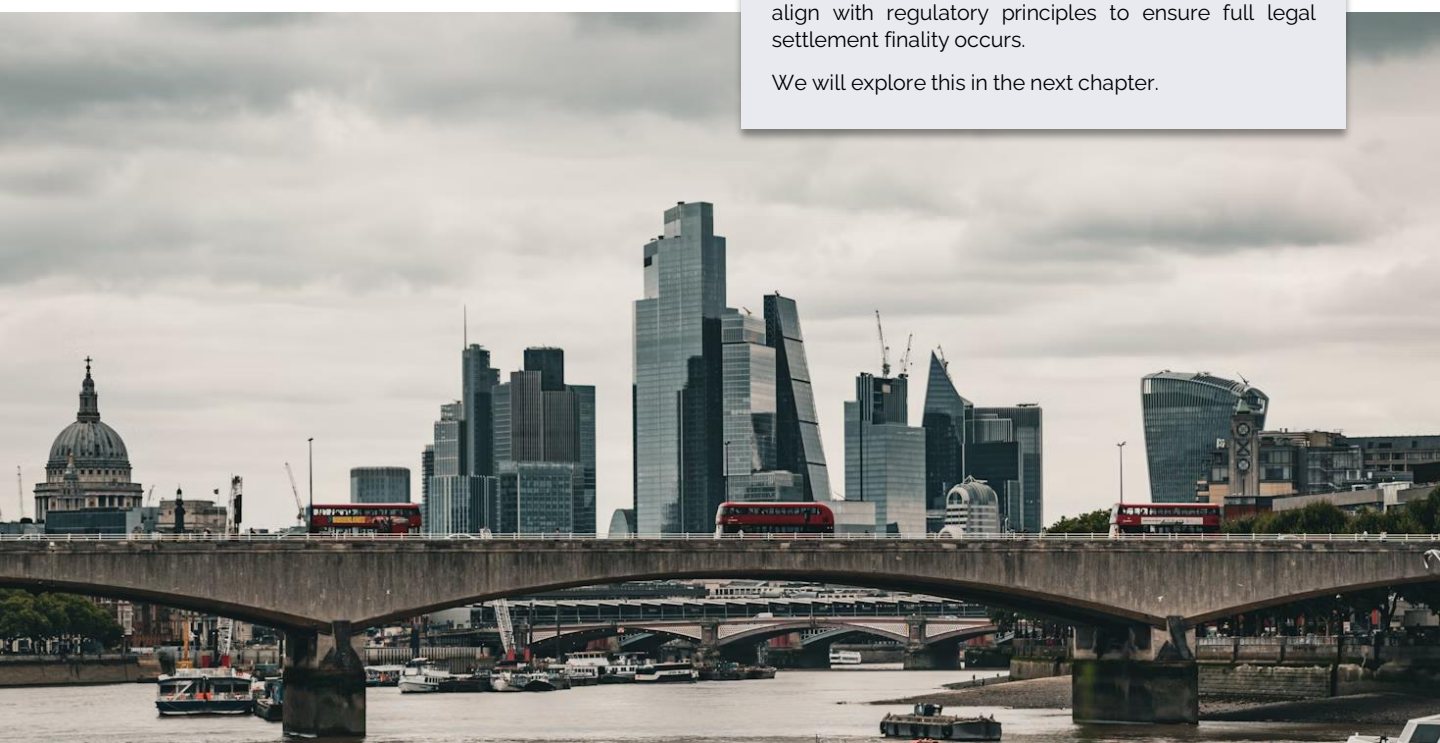
Institutions require infrastructure they can trust. They will not entrust trillions in daily transactions to self-executing code alone without safeguards, governance, and integration with the existing financial system.

Without a digital CSD, digital asset markets will struggle to mature beyond fragmented, inefficient, and high-risk settlement models.

Another critical challenge of the blockchain settlement model is the lack of legal settlement finality; an essential pillar of financial market stability.

Whilst blockchain is positioned as ensuring irrevocable and 'final' settlement, settlement infrastructure must align with regulatory principles to ensure full legal settlement finality occurs.

We will explore this in the next chapter.



In the next chapter,

*we explore why a regulated, legally enforceable framework for **settlement finality** and insolvency protection is indispensable for digital asset markets and why blockchain cannot provide it alone.*

References

3-1: https://www.nytimes.com/1974/06/29/archives/failure-of-herstatt-disturbs-banking-herstatt-failure-disturbs.html

3-2: https://www.bls.gov/data/inflation_calculator.htm

3-3: http://eprints.gla.ac.uk/95628/

3-4: https://www.lawyerdb.de/Inflationrate.aspx

3-5: https://academic.oup.com/ehr/article/129/540/1129/2769724

3-6: https://www.elliptic.co/blog/325-million-stolen-from-wormhole-defi-service

3-7: https://www.reuters.com/technology/crypto-network-wormhole-hit-with-possible-320-mln-hack-2022-02-03/

6-1: https://www.elliptic.co/blog/bybit-hack-largest-in-history

6-2: https://www.cnbc.com/2025/02/24/bybit-replenished-reserves-after-record-breaking-1point5-billion-hack.html

7-1: https://www.bitstamp.net/learn/crypto-101/what-is-block-time/

7-2: https://www.blockchain.com/explorer/charts/avg-confirmation-time

9-1: https://www.dtcc.com/~/media/Files/downloads/Thought-leadership/modernizing-the-u-s-equity-markets-post-trade-infrastructure.pdf

9-2: https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

9-3: https://chainspect.app/

9-4: https://dexola.com/blog/sui-blockchain-an-ambitious-bid-to-improve-speed-scalability-and-security/

9-5: https://ycharts.com/

9-6: https://www.dtcc.com/annuals/2023/performance

9-7: https://www.blockchain.com/explorer/charts/n-transactions

10-1: https://www.economist.com/finance-and-economics/2021/10/23/why-it-matters-when-trades-settle

10-2: https://www.coinbase.com/en-gb/learn/market-updates/around-the-block-issue-3

11-2: https://www.bankofengland.co.uk/speech/2022/september/jon-cunliffe-keynote-speech-at-the-afme-operations-post-trade-technology-innovation-conference

12-1: https://www.dtcc.com/annuals/2023/performance

17-1: https://www.coindesk.com/tech/2024/01/22/bug-on-ethereums-nethermind-software-sparks-discussion-of-client-diversity-risks

17-2: https://www.economist.com/finance-and-economics/2021/10/23/why-it-matters-when-trades-settle

17-3: https://www.spglobal.com/marketintelligence/en/mi/research-analysis/the-global-shortening-of-the-settlement-cycle-the-future-direc.html

About ClearToken

ClearToken is building a Central Counterparty (CCP) and settlement system to deliver robust financial market infrastructure to the digital asset ecosystem. This infrastructure will mitigate bilateral counterparty risk for settlement, financing, and derivative transactions by centralising clearing, collateral, and risk management arrangements. DvP settlement will also be achieved for digital assets. The systems will operate 24/7 to provide uninterrupted service while managing risk in real-time through margin and default fund contributions.

As a horizontal CCP coupled with the settlement system, ClearToken will facilitate the clearing and settlement of transactions from multiple venues and OTC markets globally. ClearToken intends to be multi-custodial and adhere to the highest AML and KYC standards. ClearToken's team comprises established corporate governance and financial markets professionals who share the objective of implementing the necessary framework for the digital asset market.

As a planned financial market infrastructure, ClearToken is seeking authorisation and recognition with the relevant regulatory bodies and will adhere to the IOSCO principles for financial market infrastructures together with all relevant legislation applicable to clearing houses, payment systems, securities and derivatives depositories, and also for virtual asset service providers.

For more information, please visit: https://cleartoken.io/

Contacts

Benjamin Santos-Stephens
CEO
ben@cleartoken.io

Niki Beattie
Chair
niki@cleartoken.io

Disclaimer

These materials have been prepared for information purposes only and do not constitute a financial promotion, an offer to sell or an inducement or solicitation of an offer to buy an interest in ClearToken Holdings Limited ("ClearToken").and should not be construed as such. Such an offer, if made, may be made only through the definitive offering documents of ClearToken, including a subscription agreement and shareholders' agreement (or similar document) which shall only be made available to persons which satisfy the criteria relevant in their local jurisdiction for such offering documents to be made available. The information contained herein is qualified in its entirety by reference to the definitive offering documents.

These materials are in summary form and have been prepared solely for informational purposes. These materials may also contain "forward-looking" statements, which can be identified by the use of forward-looking terminology such as "may," "will," "should," "expect," "anticipate," "target," "project," "estimate," "intend," "continue" or "believe," or the negatives thereof or other variations thereon or comparable terminology. Such statements are statements other than historical fact and relate to ClearToken's intent, belief or current expectations primarily with respect to its future operating, financial and strategic performance. Any such forward-looking statements, including any financial, performance or other projections, are not guarantees of future performance and may involve risks and uncertainties. Forecasted performance is subject to changes at any time and may not materialize as presented due to changes in the market or economic conditions. Actual results may differ from those contained in or implied by such statements. Neither ClearToken nor any of its directors, officers, agents or affiliates makes any representations or warranties regarding the accuracy or completeness of any projections or other forward-looking statements and assumes no responsibility to update such statements as a result of new information, future events or otherwise. Actual events, results or performance may differ materially from those reflected or contemplated by such forward-looking statements as a result of factors beyond ClearToken's control.

Forward-looking statements, including projections, included in these materials are made based on our current expectations and projections about future events and such views as they exist as of the date of publication of these materials. There is no assurance that such views are correct or will prove, with the passage of time, to be correct. Due to various risks and uncertainties, actual events or results or the actual performance of the investment may differ materially from that reflected or contemplated in these projections. Although we believe the expectations reflected in the projections are reasonable, we cannot guarantee future results, performance or achievements. Moreover, neither we nor any other person assume responsibility for the accuracy and completeness of any of these projections or have any duty to update such projections. Potential investors are cautioned not to place undue reliance on forward-looking statements.

ClearToken Services UK Limited, 1 Bow Churchyard, London EC4M 9DQ